UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	No. 5:19-cr-00535
	:	
FRANCES EDDINGS (1) and	:	
JUDE DENIS (2)	:	

O P I N I O N

Defendant Frances Eddings's Motion to Dismiss the Superseding Indictment, ECF No. 110—DENIED

Joseph F. Leeson, Jr. **June 21, 2021**
United States District Judge

I. INTRODUCTION

In this case, Defendants Jude Denis and Frances Eddings are charged with unauthorized access of a computer, exceeding authorized access of a computer, and conspiracy, in violation of the Computer Fraud and Abuse Act of 1986 ("CFAA"), 18 U.S.C. § 1030, *et seq*. The Defendants are alleged to have attempted to extort a non-profit charitable organization, the Prostate Cancer Foundation ("PCF"), through the threatened (and actual) release of documents related to PCF which Defendant Jude Denis unlawfully accessed from a computer server. Defendant Frances Eddings has moved to dismiss the Superseding Indictment under Federal Rule of Criminal Procedure 12(b)(3)(B) for failure to state an offense, a motion the Government opposes. For the reasons set forth below, Eddings's motion to dismiss is denied.

II. RELEVANT BACKGROUND

The following is a summary of the facts alleged in the Superseding Indictment ("Sup. Ind."), ECF No. 5. On August 11, 2014, Jude Denis was hired on a temporary basis by PCF to help organize an upcoming fundraising event ("the Gala"). PCF operated out of the offices of the

Philadelphia-based International Financial Company ("IFC").[1] As part of her employment with PCF, Denis was given access to IFC's email server by way of a link being loaded on her personal laptop. Approximately six days after beginning her employment with PCF, Denis resigned, claiming she had been ill-treated by the organization. However, after resigning, Denis realized she remained able to access IFC's email server.

On or around September 20, 2014, Jude Denis signed a statement authorizing Frances Eddings to act on her behalf "in all manners relating to" the PCF and IFC. Between September 22 and October 1, 2014, Denis, without authorization or permission, used the access she retained to IFC's email server to obtain documents related to PCF. Between September 30 and October 7, 2014, Eddings sent multiple emails to representatives of PCF and IFC. In these emails, Eddings threatened to release the documents unlawfully obtained by Denis from IFC's server to PFC board members, sponsors, donors, volunteers, and the media, if PCF did not pay Denis $150,000 for the mistreatment she allegedly suffered and an additional $37,500 "recovery fee" to Eddings. As threatened, on October 6 and 7 2014, Eddings sent emails to donors to the PCF Gala as well as members of the media to which were attached documents unlawfully obtained by Denis from the IFC email server.

On or about September 26, 2019, Denis and Eddings were charged by Superseding Indictment with one count of conspiracy and three counts of unlawful access of a computer, in violation of 18 U.S.C. §§ 1030(a)(2), (b).

Eddings now moves to dismiss the Superseding Indictment for failure to state an offense under Federal Rule of Criminal Procedure 12(b)(3)(B). Her argument for dismissal is grounded on the Supreme Court's recent decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021). She

[1] Denis was hired by Neil Rodin, who a member of the PCF's board and an owner of IFC.

asserts that "[t]he facts alleged in the superseding indictment fall beyond the scope of the CFAA as interpreted by *Van Buren*." Eddings's Memorandum in Support of her Motion to Dismiss ("Eddings Mem."), ECF No. 110, at 3. In particular, Eddings argues as follows:

> In this case, the parties have stipulated that Ms. Denis was given authorized access to the IFC email server on August 14, 2014 and that the access continued until October 1, 2014 when IFC changed the password. As previously discussed, "access," as defined by *Van Buren*, "turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scope-based restrictions." Thus, under *Van Buren*, Denis had authorized, "gates up" access from August 14, 2014 until October 1, 2014. The parties have stipulated that there were no failed log-in attempts made after October 1, 2014, meaning that Denis never acted as an "outside hacker" attempting to get "gates down" unauthorized access to the IFC server.
>
> Furthermore, her conduct cannot be characterized as "exceeding authorized access" under the definitions set forth in Van Buren because Denis never acted as an "internal hacker," accessing files or folders that she did not already have access to. Under *Van Buren*, her motives in accessing the information are irrelevant. Thus, the indictment fails to state a claim as to either Jude Denis or Frances Eddings.

Id. at 6.

The Government argues that Eddings misconstrues *Van Buren*'s central holding. According to the Government,

> [t]he central holding of *Van Buren*, that the "exceeds authorized access" prong does not encompass a person's improper use of information that the person was otherwise entitled to access at the time, has no application to this case. Here, the government long ago disclaimed any reliance on that now rejected legal theory. *See* Gov't Memo. in Supp. of Suppl. Jury Instr. (Docket 90-1), at pp. 5, n.1 and 9-12. Likewise, the Supreme Court's characterization of unauthorized access as applying to persons who access a computer without any permission does not affect the legal positions in this case. The government has consistently maintained that Denis' and Eddings' access was "unauthorized" because it took place after Denis terminated her employment and without the approval of her former employer. *See id*. at 5-9, 11-12 (explaining that the charged intrusions were made after Denis left her employment, and arguing that a termination of employment "forfeits any authorization to access his or her former employer's computers that may have arisen from the employment relation."). Thus, the government's theory of prosecution in this case fits comfortably with, and is entirely ratified by, *Van Buren.*

Government's Memorandum in Opposition ("Gov't. Opp'n."), ECF No. 111, at 6-7. The Government elaborates by contending that the if the facts alleged in the Superseding Indictment are proven at trial, they would establish each of the elements of the crime of unlawfully accessing a protected computer in violation of 18 U.S.C. § 1030(a)(2). *Id*. at 9. Additionally, the Government takes issue with Eddings's attempt to invoke an exception to the "no outside evidence rule" in ruling on her Rule 12 motion to dismiss, arguing that no such exception has been recognized in the Third Circuit, and even if one were, the outside "facts" she attempts to bring forward are misrepresented and not undisputed. *See id*. at 10-12. Finally, the Government argues against Eddings's claim that in *Van Buren*, the Supreme Court determined that "access" for purposes of § 1030(a)(2) "turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scoped-based restrictions." *Id*. at 13. It points out that in this quotation from *Van Buren*, (1) the Court was discussing a different section of the CFAA (the "password-trafficking" provision), and, more importantly, (2) the Court was discussing the meaning of "authentication," not "access." *See id*. at 13-14.

III. LEGAL STANDARD

As a general matter, an indictment will be deemed sufficient if it "(1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution." *United States v. Vitillo*, 490 F.3d 314, 321 (3d Cir. 2007) (quoting *United States v. Rankin,* 870 F.2d 109, 112 (3d Cir. 1989)), *as amended* (Aug. 10, 2007). A defendant can challenge the sufficiency of an indictment under Federal Rule of Criminal Procedure 12(b)(3)(B)(v) in at least two ways. *United States v. Brennan*, 452 F. Supp. 3d 225, 230 (E.D. Pa. 2020). "First, the defendant can assert that the indictment 'fails to charge an essential element of the crime.' Second, he can argue that the

'specific facts alleged . . . fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation.'" *Id*. at 230-31 (quoting *United States v. Stock*, 728 F.3d 287, 292 (3d Cir. 2013)). As with an indictment that fails to allege an essential element of a crime, an indictment that alleges facts beyond the scope of the relevant criminal statute—that is, an indictment that alleges facts which the relevant statute does not criminalize—fails to state an offense, and is insufficient as a result. *See Vitillo*, 490 F.3d at 321.

"A court's review of a motion to dismiss an indictment 'is a narrow, limited analysis geared only towards ensuring that legally deficient charges do not go to a jury.'" *Stock*, 728 F.3d at 292 n.4 (quoting *United States v. Bergrin*, 650 F.3d 257, 268 (3d Cir. 2011)). The Court is not permitted to consider the sufficiency of the government's evidence, *id*. (quoting *Berrgrin*, 650 F.3d at 265); rather, the "court [must] accept[ ] as true the factual allegations set forth in the indictment." *Bergrin*, 650 F.3d at 265 (quoting *United States v. Besmajian,* 910 F.2d 1153, 1154 (3d Cir. 1990)).

IV. DISCUSSION

Before addressing what if any impact the Supreme Court's decision in *Van Buren* has on the sufficiency of the Superseding Indictment in this matter, it is helpful to begin with the language of the relevant criminal statute. Counts two through four of the Superseding Indictment charge violations of 18 U.S.C. § 1030(a)(2).[2] Section 1030(a)(2) creates criminal liability for anyone who

> intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or

[2] Count One of the Superseding Indictment charges conspiracy under the 18 U.S.C. § 1030(b), which subsection provides that "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."

(C) information from any protected computer; . . . .

The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

In *Van Buren v. United States*, the Supreme Court addressed whether a former police officer who ran a license-plate search in a law enforcement computer database in exchange for money "exceed[ed] [his] authorized access" to obtain information from a protected computer in violation of § 1030(a)(2). *See* 141 S. Ct. 1648, 1652 (2021). Taking note of the CFAA's definition of "exceeds authorized access," the Court explained there was no dispute that Van Buren had "access[ed] a computer with authorization," and that he "obtain[ed] . . . information in the computer" when he acquired the license-plate record. *Id*. at 1654. The key dispute was "whether Van Buren was 'entitled so to obtain' the record." *Id*. After examining the arguments for competing interpretations of this phrase, the Court "agree[d] with Van Buren: The phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Id*. at 1655 (footnote omitted). The Court concluded its majority Opinion as follows:

> In sum, an individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him. The parties agree that Van Buren accessed the law enforcement database system with authorization. The only question is whether Van Buren could use the system to retrieve license-plate information. Both sides agree that he could. Van Buren accordingly did not "excee[d] authorized access" to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose.

Id. at 1662.

The Government's theory of prosecution in this case is in no way inconsistent with the holding of *Van Buren*, and Eddings's arguments to the contrary are without merit.

As an initial matter, *Van Buren*'s holding rested on the Court's statutory interpretation of liability for "exceed[ing] authorized access" under § 1030(a)(2), rather than for accessing a computer "without authorization." The Government's theory here, by contrast, has been that Denis's access to the IFC email server was "without authorization" because it took place after Denis terminated her employment with PFC. *See* Gov't. Opp'n. at 6-7; *see also* Sup. Ind., Count One ¶¶ 8-9. Nothing in *Van Buren* precludes CFAA liability premised on a theory that an individual whose employment is terminated and who accesses her previous employer's computer after such termination accesses that computer "without authorization"—which, as the Government points out, has broad support in CFAA case law. *See* Gov't Opp'n. at 15-16 (collecting cases); *see, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009) ("There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer "without authorization" for purposes of the CFAA.").

However, even where the Court in *Van Buren* discusses the interplay between liability for access "without authorization" and access that "exceeds authorization," nothing in the analysis places the Government's theory of prosecution here beyond the scope of the statute. In particular, the Supreme Court agreed with Van Buren that access "without authorization" "protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission at all.'" *Van Buren*, 141 S. Ct. at 1658 (quotation omitted). The Court went on to state that "[u]nder Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access

certain areas within the system." *Id*. at 1658-59. Why this interpretation does not doom the Government's theory of prosecution is best explained in the context of Eddings's arguments.

According to Eddings, because the parties' stipulated[3] that Denis had access to IFC's email server between August 14, 2014, and October 1, 2014, when the password was changed, under *Van Buren*, she had "authorized, 'gates up' access" during that period. ECF No. 110 at 5-6. Eddings argues that there can be no criminal liability under the access "without authorization" clause because Denis was not an "'outside hacker' attempting to get 'gates down' unauthorized access to the IFC server." *Id*. at 6. Nor, Eddings argues, was Denis an "'internal hacker,' accessing files or folders that she did not already have access to," precluding liability under the "exceeds authorized access" clause. *Id*.

However, the Government's theory of the case is that Denis was akin to an "outside hacker"—someone "who acces[sed] a computer without any permission at all." *Van Buren*, 141 S. Ct. at 1658. According to the Government, when Denis terminated her employment, she was no longer a member of or associated in any way with PFC; she was a person outside of or external to the organization and without permission to access the IFC server. *See* Gov't. Mem. at 6-7. In the Court's view, the mere fact that she retained possession of a password which allowed her to access the server post-employment does not, under *Van Buren*, mean that she necessarily was "authorized" to access the server. Rather, the issue of whether, after she terminated her employment, Denis remained authorized to access the IFC server is properly a question of fact for determination by a jury.

The argument that mere possession of the means of access of a computer system in the form of a password necessarily equates to authorization to access that computer system is incompatible

[3] The Court leaves aside the fact that Eddings asks the Court to consider facts and evidence outside the four corners of the Superseding Indictment.

with common sense as embodied in the "password-trafficking" provision of the CFAA. This provision makes it unlawful to traffic in a password "through which a computer may be accessed without authorization." 18 U.S.C. § 1030(a)(6). The Court agrees with the Government that if it is a crime to provide someone with a password by which they will be able to access a computer "without authorization," it necessarily follows that the mere possession of a password does not render any subsequent access "authorized." *See* Gov't. Opp'n. at 14-15.

V. CONCLUSION

For the reasons set forth above, the facts alleged in the Superseding Indictment do not fall beyond the scope of the CFAA as interpreted and applied by the Supreme Court in *Van Buren v. United States*. Frances Eddings's motion to dismiss the Superseding Indictment as insufficient on this basis is therefore denied.

A separate Order follows this Opinion.

BY THE COURT:

/s/ Joseph F. Leeson, Jr.
JOSEPH F. LEESON, JR.
United States District Judge